PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2004-104750
(43)Date of publication of application : 02.04.2004

(51)Int.Cl. H04L 9/32

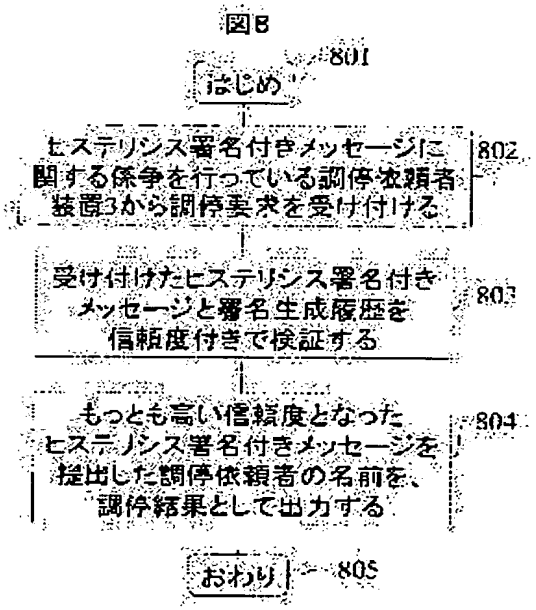
(21)Application number : 2003-022985
(22)Date of filing : 31.01.2003

(71)Applicant : HITACHI LTD
(72)Inventor : MIYAZAKI KUNIHIKO
OMOTO CHIKAHIRO
ITO SHINJI
TANIMOTO KOICHI
YOSHIURA YUTAKA

(30)Priority
Priority number : 2002207696 Priority date : 17.07.2002 Priority country : JP

(54) VERIFY METHOD OF DIGITAL SIGNATURE

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a verify method which is so constituted that the reliability of signature history may be reflected appropriately, in hysteresis signature which performs verify based on signature history, to provide a mediation method and a mediator instrument which solve dispute involving the correctness of a signature based on the verify method, and to provide a history management method which reduces load of signer's signature history management.
SOLUTION: Reliability is set in signature preparation recording which constitutes signature history. The reliability of signature history is computed from the set reliability, and computed reliability is output as the reliability of verify result. The verify method which is so constituted that the reliability of signature history may be reflected appropriately, and the mediation method and the mediator instrument which solve dispute involving the correctness of a signature can be provided. The load of storage of signature history in a signer can be reduced by installing a signature history storage service instrument.



LEGAL STATUS

[Date of request for examination] 31.01.2006

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2004-104750
(P2004-104750A)
(43)公開日　平成16年4月2日(2004.4.2)

(51)Int.Cl.[7]	F I		テーマコード（参考）
H04L 9/32	H04L 9/00	675B	5J104

審査請求 未請求　請求項の数 8　OL　（全 20 頁）

(21)出願番号　特願2003-22985(P2003-22985)
(22)出願日　平成15年1月31日(2003.1.31)
(31)優先権主張番号　特願2002-207696(P2002-207696)
(32)優先日　平成14年7月17日(2002.7.17)
(33)優先権主張国　日本国(JP)

（出願人による申告）国等の委託研究の成果に係る特許出願（平成１４年度通信・放送機構「次世代証拠基盤技術に関する研究開発」委託研究、産業活力再生特別措置法第３０条の適用を受けるもの）

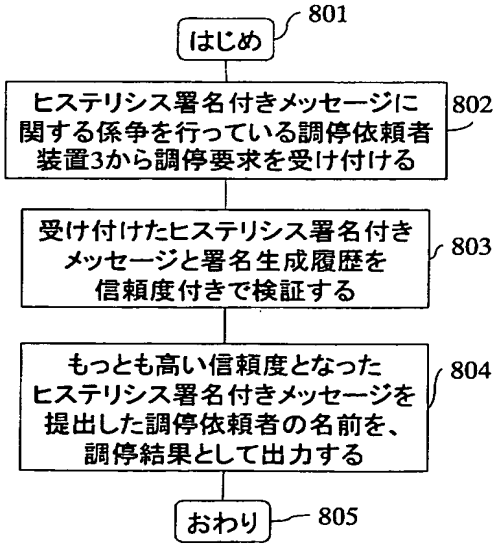
(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地
(74)代理人　100075096
弁理士　作田　康夫
(72)発明者　宮崎　邦彦
神奈川県川崎市麻生区王禅寺１０９９番地　株式会社日立製作所システム開発研究所内
(72)発明者　大本　周広
東京都江東区新砂一丁目６番２７号　株式会社日立製作所公共システム事業部内

最終頁に続く

(54)【発明の名称】ディジタル署名の検証方法

(57)【要約】
【課題】署名履歴に基づいて検証を行うヒステリシス署名において、署名履歴の信頼度を適切に反映するように構成された検証方法と、当該検証方法に基づいて署名の正当性をめぐる係争を解決する調停方法および調停者装置を提供する。また署名者の署名履歴管理の負荷を軽減する履歴管理方法を提供する。
【解決手段】署名履歴を構成する署名生成記録に信頼度を設定し、設定された信頼度から、署名履歴の信頼度を算出し、算出された信頼度を検証結果の信頼度として出力する。署名履歴の信頼度を適切に反映するように構成された検証方法や、署名の正当性をめぐる係争を解決する調停方法および調停者装置を提供可能となる。また、署名履歴保管サービス装置を設けることにより、署名者における署名履歴の保管の負荷を軽減可能となる。
【選択図】　図８

図8



【特許請求の範囲】
【請求項１】
メッセージに対するディジタル署名を検証するディジタル署名の検証方法であって、
ディジタル署名生成者側の装置において、
メッセージあるいはそのハッシュ値に、ディジタル署名生成者が所有する秘密鍵を作用させ、当該メッセージに対するディジタル署名を生成する署名生成ステップと、
生成したディジタル署名とメッセージとを含むディジタル署名付きメッセージを配布するとともに、当該ディジタル署名付きメッセージのログデータをログリストに登録する登録ステップと、を有し、
ディジタル署名検証者側の装置において、
配布されたディジタル署名付きメッセージを、検証対象ディジタル署名付きメッセージとして受け付ける検証対象受付ステップと、
前記検証対象ディジタル署名付きメッセージを配布したディジタル署名者のログリストを取得する履歴取得ステップと、
前記検証対象ディジタル署名付きメッセージのログデータが、前記ログリストに登録されているか否かを調べる履歴有無検証ステップとを備え、
登録されている場合は、さらに、前記ログリストに含まれるログデータの信頼度を設定する個別信頼度設定ステップと、
設定された個別信頼度から前記ログリストの信頼度を算出する履歴信頼度算出ステップと、
当該検証対象ディジタル署名付きメッセージが前記ディジタル署名生成者側装置により配布されたものであることを、信頼度付きで認証する検証ステップと、を有することを特徴とするディジタル署名の検証方法。
【請求項２】
メッセージに対するディジタル署名に関する係争を解決する調停方法であって、
調停において、
調停依頼者装置から調停対象となるディジタル署名付きメッセージを受け付ける要求受付ステップと、
前記調停対象となるディジタル署名付きメッセージに関するログリストを入手する履歴入手ステップと、
請求項１記載の検証ステップと、
前記検証ステップの出力である信頼度に基づき、調停結果を出力する調停ステップと、
を有することを特徴とする調停方法。
【請求項３】
ディジタル署名の検証装置であって、
検証対象となるディジタル署名付きメッセージを受け付ける検証対象受付手段と、
前記検証対象ディジタル署名付きメッセージを配布したディジタル署名者のログリストを取得する履歴取得手段と、
前記検証対象ディジタル署名付きメッセージのログデータが、前記ログリストに登録されているか否かを調べる履歴有無検証手段と、
前記登録がされている場合は、前記ログリストに含まれるログデータの信頼度を設定する個別信頼度設定手段と、
設定された個別信頼度から前記ログリストの信頼度を算出する履歴信頼度算出手段と、
当該検証対象ディジタル署名付きメッセージが前記ディジタル署名生成者側装置により配布されたものであることを、信頼度付きで認証する検証手段と、
を備えることを特徴とするディジタル署名の検証装置。
【請求項４】
メッセージに対するディジタル署名に関する係争を解決する調停者装置であって、
調停対象となるディジタル署名付きメッセージを受け付ける要求受付手段と、前記調停対象となるディジタル署名付きメッセージに関するログリストを取得する履歴取得手段と、

前記調停対象ディジタル署名付きメッセージのログデータが、前記ログリストに登録されているか否かを調べる履歴有無検証手段と、
前記登録がされている場合は、前記ログリストに含まれるログデータの信頼度を設定する個別信頼度設定手段と、
設定された個別信頼度から前記ログリストの信頼度を算出する履歴信頼度算出手段と、
前記信頼度に基づき、調停結果を出力する調停手段と、
を備えることを特徴とする調停者装置。
【請求項５】
ディジタル署名生成者が使用するディジタル署名生成者側装置がメッセージに対して作成するディジタル署名の生成履歴であるログリストを、ログリスト保管側装置において管理する方法であって、
前記ディジタル署名生成者側装置において、
前記ログリスト保管者側装置に対して、前記ログリストの登録を要求するステップを有し、
前記ログリスト保管者側装置において、
前記ディジタル署名生成者側装置から前記ログリストを受け付けるステップと、
当該ログリストまたはログリスト登録要求データに付された前記ディジタル署名者のディジタル署名の有効性を検証するステップと、
受け付けた前記ログリストと、登録されている前記ディジタル署名者の登録済みログリストとの整合性を検証するステップと、
前記整合性を確認した前記ログリストを前記ディジタル署名者の前記登録済みログリストに追記するステップと、
を有することを特徴とするログリストの管理方法。
【請求項６】
請求項５に記載のログリストの管理方法であって、
前記ログリスト保管者側装置において、
前記整合性を確認し、前記ログリストを前記ディジタル署名者の前記登録済みログリストに追記したこと前記ディジタル署名者側装置へ通知するステップと、
前記ディジタル署名者側装置において、
前記ログリストに含まれる最新のログデータを除く他のログデータを削除するステップと、
を有することを特徴とするログリストの管理方法。
【請求項７】
ディジタル署名生成者が使用するディジタル署名生成者側装置が、メッセージに対して作成してディジタル署名受信者側装置へ送信したディジタル署名を、ログリスト保管者側装置が検証するディジタル署名の検証方法であって、
前記ディジタル署名生成者側の装置において、
メッセージあるいはそのハッシュ値に、前記ディジタル署名生成者が所有する秘密鍵を作用させ、当該メッセージに対するディジタル署名を生成する署名生成ステップと、
生成した前記ディジタル署名と前記メッセージとを含むディジタル署名付きメッセージを前記ディジタル署名受信者側装置へ送信するとともに、当該ディジタル署名付きメッセージのログデータをログリストに登録する登録ステップと、
前記ログリスト保管者側装置に対して、前記ログリストの登録を要求するステップを有し、
前記ディジタル署名受信者側装置において、
前記ディジタル署名付きメッセージを受信するステップと、
前記ログリスト保管者側装置に対して、当該ディジタル署名付きメッセージの検証代行を依頼するステップを有し、
前記ログリスト保管者側装置において、
前記ディジタル署名生成者側装置から前記ログリスト登録要求を受け付けるステップと、

前記ログリスト登録要求に含まれる前記ログリストまたは当該ログリスト登録要求に付された、前記ディジタル署名者が生成したディジタル署名の有効性を検証するステップと、
受け付けた前記ログリストと、既に登録済みの当該ディジタル署名者のログリストとの整合性を検証するステップと
前記ディジタル署名受信者側装置から前記ディジタル署名受信者側装置が受信した前記ディジタル署名付きメッセージの検証依頼を受け付けるステップと、
前記登録済みの前記ディジタル署名者のログリストを用いて、当該検証を依頼された前記ディジタル署名付きメッセージが、前記ディジタル署名生成者側装置により生成されたものであることを認証する検証ステップと、
を有することを特徴とするログリストの管理方法。

【請求項８】
ディジタル署名生成者が使用するディジタル署名生成者側装置が、メッセージに対して作成してディジタル署名受信者側装置へ送信したディジタル署名を検証するログリスト保管者側装置であって、
前記ディジタル署名生成者側装置からログリスト登録要求を受け付ける手段と、
前記ログリスト登録要求に含まれる前記ログリストまたは当該ログリスト登録要求に付された、前記ディジタル署名者が生成したディジタル署名の有効性を検証する手段と、
受け付けた前記ログリストと、既に登録済みの当該ディジタル署名者のログリストとの整合性を検証する手段と
前記ディジタル署名受信者側装置から前記ディジタル署名受信者側装置が受信した前記ディジタル署名付きメッセージの検証代行依頼を受け付ける手段と、
前記登録済みの前記ディジタル署名者のログリストを用いて、当該検証代行を依頼された前記ディジタル署名付きメッセージが、前記ディジタル署名生成者側装置により生成されたものであることを認証する検証手段と、
を有することを特徴とするログリスト保管者側装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】
本発明は情報セキュリティに関する。

【０００２】

【従来の技術】
電子署名の安全性を高める技術として、署名生成時にその記録を履歴として残しておき、また、新たに署名を生成する際には、その時点における履歴データを反映させることにより、署名間に論理的な連鎖関係を構築する技術（これをヒステリシス署名と呼ぶ）がある。

【０００３】
上記ヒステリシス署名技術については、特許文献１などに開示されている。

【０００４】
また、信頼できる第三者機関が文書の作成、送信等の否認防止のためのサービスを提供する技術が、たとえば、非特許文献１などに開示されている。

【０００５】

【特許文献１】
特開２００１－３３１１０４号公報

【非特許文献１】
ＩＳＯ（the International Organization for Standardization）and ＩＥＣ（the International Electrotechnical Commission），”ＩＮＴＥＲＮＡＴＩＯＮＡＬ ＳＴＡＮＤＡＲＤ ＩＳＯ／ＩＥＣ １３８８８－２ Information technology － Security techniques － Non－repudiation －Part 2: Mechanisms using

symmetric techniques", first edition, (スイス), 1998.4.1

【0006】

【発明が解決しようとする課題】

上記ヒステリシス署名技術では、署名の検証を行う際に、当該に関する署名履歴を利用している。したがって、この署名履歴の信頼度を適切に反映するように構成されたヒステリシス署名の検証方法が望まれている。

【0007】

また、上記ヒステリシス署名により生成された署名履歴を長期にわたり保管することは、一般的な署名者や、署名者側装置にとっては負担が大きい。したがって、一般利用者の署名履歴保管の負荷を軽減する保管方法が望まれている。

【0008】

また、非特許文献1は、信頼できる第三者機関に対し送られてきた保証対象データに対して、その存在を保証するトークンを生成して返送する否認防止サービスを開示しており、データの保管については述べていない。また、上記サービスは、ヒステリシス署名の有効性を保証するためのサービスとしては、保証対象データとなる署名履歴のチェック方法などに不十分な点がある。

【0009】

【課題を解決するための手段】

本発明は、署名履歴の信頼度を適切に反映するように構成されたヒステリシス署名の検証方法を提供する。

【0010】

また、本発明は、署名者側装置に代わり署名履歴（署名生成履歴ともいう）を長期にわたり信頼性の高い状態で保管し、署名者側装置の署名履歴保管の負荷を軽減する署名履歴保管サービスを実現する技術を提供する。

【0011】

さらに、署名履歴保管サービス提供者側装置は、署名者側装置から登録を要求された署名履歴データに対して、登録要求時点において、当該署名者側装置が過去に生成し署名履歴保管サービス提供者側装置が既に保管済みのデータとの整合性を検証し、または、当該署名者用の公開鍵証明書の有効性検証を含む署名検証処理を行うことにより、その時点での署名履歴の正当性を確認してから、実際に署名履歴を保管する。これらのどちらか、または、両方のステップによって、たとえ長期経過後であってもヒステリシス署名の有効性をより確実に検証可能となる。

【0012】

また、本発明は、ヒステリシス署名つきメッセージを保持する利用者である署名検証代行依頼者からの依頼をうけ検証処理を代行する、署名検証代行サービスを実現する技術を提供する。

【0013】

本発明の一態様によれば、ヒステリシス署名検証において、検証に利用される署名生成履歴（ログリストという）に含まれる各署名生成記録（ログデータという）に対し個別信頼度を設定し、個別信頼度から署名生成履歴の信頼度を算出し、これを検証結果の信頼度として出力する、ヒステリシス署名の検証方法を提供する。

【0014】

また本発明の一態様によれば、ある署名の真偽をめぐって二者（あるいはそれ以上）の間で係争が起こったときに、上記ヒステリシス署名の検証方法にしたがって出力された検証結果の信頼度に基づき、調停結果を出力する調停方法を提供する。

【0015】

また本発明の他の態様によれば、署名履歴保管サービスが提供される。このサービスによれば、署名者は、作成したログデータを、ログデータが作成されるたび、あるいは、いくつかのログデータが作成された後の定期的あるいは不定期的なある時点に、署名履歴保管

サービス提供者側装置である履歴管理装置にログデータを預託することができる。また、依頼を受けた署名履歴保管サービス提供者は、履歴管理装置を用いて、預託されたログデータの正当性（既預託分との整合性、預託時点における署名の有効性、など）を検証し保管する。

【００１６】

また本発明の他の態様によれば、さらに、署名検証代行サービス、が提供される。このサービスによれば、ヒステリシス署名つきメッセージの所有者が使用する署名検証代行依頼者側装置からの署名検証代行依頼に応じて、署名履歴保管サービス提供者が、自らの履歴管理装置が保持する、当該ヒステリシス署名つきメッセージの署名者の署名生成履歴を用いて、ヒステリシス署名つきメッセージの正当性を検証する。

【００１７】

なお、本発明において、メッセージとは、ディジタル署名を施す対象となるディジタルデータを指す。

【００１８】

【発明の実施の形態】

図１は、本発明の第１実施形態が適用されたシステムの概略図である。

【００１９】

図示するように、ネットワーク５を介して、ヒステリシス署名を生成する署名者が利用する装置である署名者装置１と、前記署名者装置１において生成された署名生成履歴を管理する履歴管理装置２と、前記署名者が生成した署名の正当性に関し調停を依頼する調停依頼者が利用する調停依頼者装置３と、依頼に応じて署名の正当性判定を行い調停する調停者装置４とが接続されている。なお図１には、それぞれの装置が一台ずつ存在する場合を示しているが、一般には複数存在していてよい。

【００２０】

図２は、署名者装置１の概略構成を示した図である。

【００２１】

署名者装置１は、ＣＰＵ１１と、ＣＰＵ１１のワークエリアとして機能するＲＡＭ１２と、ハードディスク装置などの外部記憶装置１３と、ＣＤ－ＲＯＭやＦＤなどの可搬性を有する記憶媒体１５からデータを読取る読取り装置１４と、キーボードやマウスなどの入力装置１６と、ディスプレイなどの表示装置１７と、ネットワークを介して他の装置と通信を行うための通信装置１８と、上述した各構成要素間のデータ送受を司るインターフェイス２０を備えた、一般的な構成を有する電子計算機２１で構築することができる。

【００２２】

署名者装置１の外部記憶装置１３に格納されるのは、メッセージに対するディジタル署名を生成し、生成されたディジタル署名（ヒステリシス署名）を付したヒステリシス署名付きメッセージを配布し、また、履歴管理装置２に対し署名生成記録の登録を依頼するための、署名付きメッセージ作成ＰＧ（プログラム）１３１である。これは、ＲＡＭ１２上にロードされ，ＣＰＵ１１により、署名付きメッセージ作成処理部１１１というプロセスとして具現化される。

【００２３】

履歴管理装置２、調停依頼者装置３、調停者装置４も署名者装置１と同様の構成を備える。

【００２４】

履歴管理装置２の外部記憶装置１３に格納されるのは、署名者装置１から登録を依頼された署名生成記録を受信し、当該署名生成記録を署名履歴として登録する履歴登録ＰＧ（プログラム）１３２と、署名者装置１や、調停依頼者装置３や、調停者装置４からの要求に応じて、自履歴管理装置２が管理する署名履歴を送信する履歴送信ＰＧ（プログラム）１３３である。これらは、ＲＡＭ１２上にロードされ、ＣＰＵ１１により履歴登録処理部１１２や履歴送信処理部１１３というプロセスとして具現化される。

【００２５】

調停依頼者装置３の外部記憶装置１３に格納されるのは、調停対象となるヒステリシス署名付きメッセージに関する署名履歴を履歴管理装置２に要求し受信する履歴要求ＰＧ（プログラム）１３４と、調停対象となるヒステリシス署名付きメッセージとそれに関する署名履歴を調停者装置４に送信し、調停を依頼する調停依頼ＰＧ（プログラム）１３５である。これは、ＲＡＭ１２上にロードされ、ＣＰＵ１１により履歴要求処理部１１４や調停依頼処理部１１５というプロセスとして具現化される。

【００２６】

調停者装置４の外部記憶装置１３に格納されるのは、各調停依頼者装置３からヒステリシス署名付きメッセージとそれに関する署名履歴を受信し、最も信頼度の高い調停依頼者を判定する調停ＰＧ（プログラム）１３６である。これらは、ＲＡＭ１２上にロードされ、ＣＰＵ１１により調停処理部１１６というプロセスとして具現化される。

【００２７】

各プログラムは、予め外部記憶装置１３に格納されていても良いし、必要に応じて、読取り装置１４を介して記憶媒体１５から、または通信装置１８とネットワークを介して、他の装置から導入されても良い。

【００２８】

本実施例においては、署名者装置１、履歴管理装置２、調停依頼者装置３、調停者装置４を、それぞれ独立した装置としているが、これと異なっていてもよい。たとえば、署名者装置１の機能と履歴管理装置２の機能が同一装置上で実現されていてもよい。この場合、署名者の署名生成記録を署名者自身によって管理できるため、履歴管理装置２に対し署名生成記録の登録を依頼する必要がなくなる。

【００２９】

あるいは、履歴管理装置２の機能と調停者装置４の機能を同一装置上に実現してもよい。この場合、調停依頼者が調停者装置４に対し、調停を依頼するときに、事前に調停対象となるヒステリシス署名付きメッセージに関する署名履歴を入手する必要がなくなるため、効率的である。また、通常、取引の際には、双方向でデータがやり取りされることを考えると、同一人が、ある場面においては署名者であり、別の場面においては調停依頼者となることも考えられる。このような場合には、署名者装置１の機能と調停依頼者装置３の機能を同一装置上に実現すればよい。

【００３０】

なお、本実施例においては、署名者装置１が複数台存在する場合には、履歴管理装置２は、それら複数の署名者装置１の署名生成記録を管理するようにしてもよい。このような複数の署名者装置１の署名生成履歴を管理する場合については、後述の第２実施形態の説明において、署名履歴保管サービス装置として、詳しく述べる。

【００３１】

図３は、署名者装置１の署名付きメッセージ作成ＰＧ１３１の処理フローを示す。

ステップ３０１：はじめ。

ステップ３０２：署名対象メッセージを作成する。

ステップ３０３：署名対象メッセージに対しヒステリシス署名を生成する。

ステップ３０４：ステップ３０３で生成された署名に関する署名生成記録（ログデータ）を履歴管理装置２に送る（登録を依頼する）。

ステップ３０５：（必要であれば）ヒステリシス署名付きメッセージを公開鍵証明書をつけて受信者装置に送る。

ステップ３０６：おわり。

【００３２】

なお、ステップ３０５における受信者装置は、図１には図示されていない。たとえば、署名対象メッセージが、取引契約書である場合、当該契約書の受け取り手である取引相手の装置がこれに該当する。受信者装置の概略構成は、図２と同様でよい。また、調停依頼者が受信者となり、調停依頼者装置と受信者装置とが同じであっても良い。

【００３３】

また、ステップ３０３におけるヒステリシス署名の生成は、具体的には以下に示す「ヒステリシス署名生成処理」の手順に従って実現可能である。なお説明にあたっては、以下の記法を用いる。また、署名者をＡｌｉｃｅと称することにする。

【００３４】

「記法」

Ｓｉｇｎ＿Ｋ（）　：　署名生成鍵Ｋを用いた、従来の電子署名方法（例：ＲＳＡ署名、ＤＳＡ署名、ＥＣＤＳＡ署名など）における署名生成処理

Ｖｅｒｉｆｙ＿Ｋ（）　：　署名検査鍵Ｋを用いた、従来の電子署名方法における署名検査処理

ｈ（）　：　一方向性ハッシュ関数（例：ＳＨＡ－１ハッシュ関数、ＭＤ５ハッシュ関数など）

Ａ｜｜Ｂ　：　二つのデータＡ，Ｂを連結したデータ

Ｋｓ　：　Ａｌｉｃｅの署名生成鍵

Ｋｖ　：　Ａｌｉｃｅの署名検査鍵

ｎ　：　Ａｌｉｃｅがヒステリシス署名生成を行った回数

ＩＶ　：　初期値

Ｍｎ　：　ｎ　番目の署名対象メッセージ

Ｓｎ　：　ｎ　番目のヒステリシス署名付きメッセージ

Ｒｎ　：　ｎ　番目のヒステリシス署名生成記録

Ｈｎ　：　ｎ　回目のヒステリシス署名生成を行った後の署名生成履歴（１　回目からｎ　回目までのヒステリシス署名生成記録を連結したデータ。

【００３５】

「ヒステリシス署名生成処理」

ステップ３０３１：（署名生成フェーズ）署名対象メッセージＭｎのハッシュ値ｈ（Ｍｎ）を算出する。

ステップ３０３２：保存してある署名生成履歴Ｈｎ－１に含まれる最新の署名生成記録Ｒｎ－１のハッシュ値ｈ（Ｒｎ－１）を算出する。ただし，１回目のヒステリシス署名生成処理においては，以降の手順でハッシュ値ｈ（Ｒｎ－１）の代わりに初期値ＩＶを用いる。

ステップ３０３３：ステップ３０３１、３０３２で算出した二つのハッシュ値を連結したデータ

ｈ（Ｍｎ）｜｜ｈ（Ｒｎ－１）に対して，署名生成鍵Ｋｓを用いて従来の署名生成処理を行い，電子署名付きメッセージ

Ｓｉｇｎ＿Ｋｓ（ｈ（Ｍｎ）｜｜ｈ（Ｒｎ－１））を生成する。

ステップ３０３４：署名対象メッセージＭｎ，最新の署名生成記録のハッシュ値ｈ（Ｒｎ－１），および電子署名付きメッセージ

Ｓｉｇｎ＿Ｋｓ（ｈ（Ｍｎ）｜｜ｈ（Ｒｎ－１））を連結し，ヒステリシス署名付きメッセージ

Ｓｎ＝Ｍｎ｜｜ｈ（Ｒｎ－１）｜｜Ｓｉｇｎ＿Ｋｓ（ｈ（Ｍｎ）｜｜ｈ（Ｒｎ－１））を生成する。

ステップ３０３５：（署名生成履歴更新フェーズ）二つのハッシュ値ｈ（Ｍｎ），ｈ（Ｒｎ－１）と電子署名付きメッセージ

Ｓｉｇｎ＿Ｋｓ　（ｈ（Ｍｎ）｜｜ｈ（Ｒｎ－１））とを連結し，署名生成記録

Ｒｎ＝ｈ（Ｍｎ）｜｜ｈ（Ｒｎ－１）｜｜Ｓｉｇｎ＿Ｋｓ（ｈ（Ｍｎ）｜｜ｈ（Ｒｎ－１））を生成する。

ステップ３０３６：保存してある署名生成履歴Ｈｎ－１と署名生成記録Ｒｎとを連結し，署名生成履歴

Ｈｎ＝Ｈｎ－１｜｜Ｒｎを生成して保存する。

【００３６】

なお上記ステップ３０３１では、署名対象メッセージＭｎのハッシュ値ｈ（Ｍｎ）を算出

しているが、署名生成処理Ｓｉｇｎ＿Ｋ（）が許容するのであれば、以降の処理で、ハッシュ値のかわりに、署名対象メッセージＭｎそのものを用いてもよい。署名生成処理Ｓｉｇｎ＿Ｋ（）が許容する例としては、たとえば、入力データ長にあわせて署名生成処理Ｓｉｇｎ＿Ｋ（）を繰り返し適用することにより任意長のデータを許容可能とする方法などがある。

【００３７】

また、上記のヒステリシス署名生成方法では、Ａｌｉｃｅがヒステリシス署名生成を行った回数ｎ、つまり、ある署名生成記録が何番目の署名生成記録であるかを示すインデックスが、署名生成記録に明示的には含まれていない。

【００３８】

しかし、以下に示す方法を用いて、上記インデックスが含まれるようにしてもよい。たとえば、ステップ３０３３での署名対象メッセージとして、

ｈ（Ｍｎ）｜｜ｈ（Ｒｎ－１）の代わりに、

ｈ（Ｍｎ）｜｜ｈ（Ｒｎ－１）｜｜ｎを使うようにし、ステップ３０３４でのヒステリシス署名付きメッセージ

Ｓｎ＝Ｍｎ｜｜ｈ（Ｒｎ－１）｜｜Ｓｉｇｎ＿Ｋｓ（ｈ（Ｍｎ）｜｜ｈ（Ｒｎ－１））の代わりに、

Ｓｎ＝Ｍｎ｜｜ｈ（Ｒｎ－１）｜｜Ｓｉｇｎ＿Ｋｓ（ｈ（Ｍｎ）｜｜ｈ（Ｒｎ－１）｜｜ｎ）｜｜ｎとし、また、署名生成記録

Ｒｎ＝ｈ（Ｍｎ）｜｜ｈ（Ｒｎ－１）｜｜Ｓｉｇｎ＿Ｋｓ（ｈ（Ｍｎ）｜｜ｈ（Ｒｎ－１））の代わりに、

Ｒｎ＝ｈ（Ｍｎ）｜｜ｈ（Ｒｎ－１）｜｜Ｓｉｇｎ＿Ｋｓ（ｈ（Ｍｎ）｜｜ｈ（Ｒｎ－１）｜｜ｎ）｜｜ｎとすればよい。

上記のように処理することにより、署名検証処理等において、署名生成履歴中から必要な署名生成記録を検索することが容易になる。

【００３９】

図４は、履歴管理装置２の履歴登録ＰＧ１３２の処理フローを示す。

ステップ４０１：はじめ。

ステップ４０２：署名者装置１から署名生成記録を受信する（登録依頼を受け付ける）。（署名者をＡｌｉｃｅとする）

ステップ４０３：すでに登録済みのＡｌｉｃｅの署名生成履歴（ログリスト）との整合性をチェックし整合していればステップ４０５へ。そうでなければ４０４へ。

ステップ４０４：「登録失敗」という結果を署名者装置１に返し、おわり。

ステップ４０５：ステップ４０２で受け付けた署名生成記録をＡｌｉｃｅの署名生成履歴に追記する。

ステップ４０６：「登録成功」という結果を署名者装置１に返す。

ステップ４０７：おわり。

【００４０】

なお、ステップ４０３における整合性のチェックは、具体的には以下のようにして実現可能である。なお、ステップ４０２で受信した署名生成記録Ｈｎとし、ステップ４０３の時点ですでに登録済みのＡｌｉｃｅの署名生成履歴をＨｎ－１とする。

【００４１】

まず、署名生成履歴をＨｎ－１のなかの最新の署名生成記録Ｈｎ－１のハッシュ値ｈ（Ｈｎ－１）を算出する。次に、算出したハッシュ値ｈ（Ｈｎ－１）が、ステップ４０２で受信した署名生成記録Ｈｎの中のハッシュ値ｈ（Ｈｎ－１）と一致するか否かを確認する。一致すれば、整合していると判定し、そうでなければ整合していないと判定する。

【００４２】

図５は、履歴管理装置２の履歴送信ＰＧ１３３の処理フローを示す。

ステップ５０１：はじめ。

ステップ５０２：履歴送信要求（署名者名、要求履歴範囲（何番目から何番目までか）な

どを含む）を受け付ける。
ステップ５０３：要求を受け付けた範囲の署名生成記録からなる署名生成履歴を要求者に送信する。
ステップ５０４：おわり。
【００４３】
図６は、調停依頼者装置３の履歴要求ＰＧ１３４の処理フローを示す。
ステップ６０１：はじめ。
ステップ６０２：調停依頼対象となるヒステリシス署名付きメッセージに関する署名生成履歴の送信を、履歴管理装置２に要求する。（当該ヒステリシス署名の署名者名、要求範囲（例：当該ヒステリシス署名に関する署名生成記録から、現時点での最新の署名生成記録までの全ての署名生成記録からなる署名生成履歴）を送る。）
ステップ６０３：履歴管理装置２から、署名生成履歴を受信する。
ステップ６０４：おわり。
【００４４】
図７は、調停依頼者装置３の調停依頼ＰＧ１３５の処理フローを示す。
ステップ７０１：はじめ。
ステップ７０２：調停者装置４に対し、調停依頼対象となるヒステリシス署名付きメッセージと、履歴管理装置２から入手した、当該ヒステリシス署名付きメッセージに関する署名生成記録を含む署名生成履歴を送信し、調停を依頼する。
ステップ７０３：調停結果を受信する。
ステップ７０４：おわり。
【００４５】
図８は、調停者装置４の調停ＰＧ１３６の処理フローを示す。
ステップ８０１：はじめ。
ステップ８０２：ヒステリシス署名付きメッセージに関する係争を行っている調停依頼者が使用する調停依頼者装置３（一般には複数）から調停要求を受け付ける。
ステップ８０３：それぞれの調停依頼者装置３から受け付けたヒステリシス署名付きメッセージと署名生成履歴を信頼度付きで検証する。ステップ８０４：もっとも高い信頼度となったヒステリシス署名付きメッセージを提出した調停依頼者の名前を、調停結果として出力する。（調停依頼者装置３達に送信する）
ステップ８０５：おわり。
【００４６】
なお、上記ステップ８０３における検証処理は、具体的には以下に示す「ヒステリシス署名検証処理」の手順に従って実現可能である。
【００４７】
「ヒステリシス署名検証処理」
まず、ヒステリシス署名付きメッセージＳｎの検証を、次のように行う。
ステップ８０３１：ヒステリシス署名付きメッセージＳｎに含まれる署名対象メッセージＭｎのハッシュ値ｈ（Ｍｎ）を算出する。
ステップ８０３２：ステップ８０３１で算出したハッシュ値ｈ（Ｍｎ）と、ヒステリシス署名付きメッセージＳｎに含まれるハッシュ値ｈ（Ｒｎ－１）および電子署名付きメッセージＳｉｇｎＫｓ（ｈ（Ｍｎ）｜｜ｈ（Ｒｎ－１））
と、Ａｌｉｃｅ　の公開鍵証明書に含まれる署名検査鍵Ｋｖとを用いて従来の署名検証処理を行う。検証できなければ検証失敗として終了。
ステップ８０３３：Ａｌｉｃｅの署名生成履歴Ｈｎのなかに、検証対象となっているヒステリシス署名付きメッセージに対応する署名生成記録
Ｒｍ＝ｈ（Ｍｍ）｜｜ｈ（Ｒｍ－１）｜｜ＳｉｇｎＫｓ（ｈ（Ｍｎ）｜｜ｈ（Ｒｍ－１））
が含まれていることを確認する。確認できなければ、検証失敗として終了。
ステップ８０３４：ｋ＝ｍとし、以下の署名生成履歴Ｈｎの整合性検証を行う。

（ｉ）署名生成履歴Ｈｎに含まれる署名生成記録Ｒｋ－１のハッシュ値ｈ（Ｒｋ－１）を算出する。
（ｉｉ）署名生成記録Ｒｋの中のハッシュ値ｈ（Ｒｋ－１）が、上で算出したｈ（Ｒｋ－１）と同じ値であることを確認する。確認できなければ、ステップ８０３５へ。
（ｉｉｉ）ｋ＜ｎであれば、ｋ：＝ｋ＋１とし、（ｉ）へ。そうでなければ、ステップ８０３５へ。
ステップ８０３５：署名生成履歴Ｈｎのうち整合性が確認できた署名生成記録Ｒｍ，．．．，Ｒｋについて、それぞれの信頼度を設定する。
ステップ８０３６：ステップ８０３５で設定された各署名生成記録の信頼度から、検証対象となる署名に対応する署名生成記録Ｒｍの信頼度を算出し、これを検証結果（「検証成功」）の信頼度として出力する。

【００４８】

なお、上記のステップ８０３５で設定する署名生成記録の信頼度は、たとえば、次に述べる個別信頼度とすればよい。

【００４９】

署名生成記録Ｒｉ　の個別信頼度とは，Ｒｉ　の検査手順によって決まる値
ｆ＿ｒｅｌｙ（Ｒｉ）　＝　（ｐｉｎｄ（Ｒｉ），　ｑｉｎｄ（Ｒｉ），　ｔｉｎｄ（Ｒｉ））　のことである。ただし，
ｐｉｎｄ（Ｒｉ），　ｑｉｎｄ（Ｒｉ），　ｔｉｎｄ（Ｒｉ）　は，他の署名生成記録とは独立に，以下で定義される。
ｐｉｎｄ（Ｒｉ）：Ｒｉ　が正当であるとき，当該検査手順によって「正当」と判定される確率
（１／２　＜＝　ｐｉｎｄ（Ｒｉ）　＜＝　１）
ｑｉｎｄ（Ｒｉ）：Ｒｉ　が偽造であるとき，当該検査手順によって「正当」と判定される確率
（０　＜＝　ｑｉｎｄ（Ｒｉ）　＜＝　１／２）
ｔｉｎｄ（Ｒｉ）：当該検査手順によるＲｉ　の判定結果（Ｒｉ　が「正当」と判定されたときｔｉｎｄ（Ｒｉ）　＝　１，　Ｒｉ　が「偽造」と判定されたときｔｉｎｄ（Ｒｉ）　＝　０）
なお、判断材料がない等の理由により、ある署名生成記録Ｒｉ　の検査ができない場合には、個別信頼度は、
ｆ＿ｒｅｌｙ（Ｒｉ）　＝（１／２，　１／２，　１）　と設定するものとする。

【００５０】

また、上記のステップ８０３６で算出する検証対象となる署名に対応する署名生成記録Ｒｍの信頼度とは、たとえば次にのべる署名生成履歴の信頼度とすればよい。

【００５１】

署名生成履歴Ｈｎ　の署名生成記録Ｒｍ　に関する信頼度とは、Ｒｍ　が実際に正当である確率ｆ＿ｐｏｓｔ＿ｒｅｌｙ（Ｒｍ）　のことである。ｆ＿ｐｏｓｔ＿ｒｅｌｙ（Ｒｍ）については、次の命題が成り立つ。

【００５２】

（命題１）
ｆ＿ｐｏｓｔ＿ｒｅｌｙ（Ｒｍ）＞＝Π＿｛ｉ＝ｍ，，，ｋ｝　Ｐｉｎｄ（Ｒｉ）　／（Π＿｛ｉ＝ｍ，，，ｋ｝　Ｐｉｎｄ（Ｒｉ）　＋　Π＿｛ｉ＝ｍ，，，ｋ｝　Ｑｉｎｄ（Ｒｉ））…（式１）
（ただし、Π＿｛ｉ＝ｍ，，，ｋ｝　Ｘｉ　は、ＸｍからＸｋまでの総積をあらわす。すなわち、Π＿｛ｉ＝ｍ，，，ｋ｝　Ｘｉ　＝　Ｘｍ×…×Ｘｋである。Ｐｉｎｄ（Ｒｉ）は、ｔｉｎｄ（Ｒｉ）＝１の時はｐｉｎｄ（Ｒｉ）、ｔｉｎｄ（Ｒｉ）＝０の時は１－ｐｉｎｄ（Ｒｉ）で、Ｑｉｎｄ（Ｒｉ）は、ｔｉｎｄ（Ｒｉ）＝１の時はｑｉｎｄ（Ｒｉ）、ｔｉｎｄ（Ｒｉ）＝０の時は１－ｑｉｎｄ（Ｒｉ）とする。）
が成り立つ。

【００５３】
（証明の概略）今、署名生成記録Ｒｉ　とＲｉ＋１　が連鎖しているとし、それぞれ適切な検査手順によって正当であると判定されたとする。すなわち、
ｆ＿ｒｅｌｙ（Ｒｊ）　＝　（ｐｉｎｄ（Ｒｊ），　ｑｉｎｄ（Ｒｊ），　１）　（ｊ＝ｉ，　ｉ＋１）　であったとする。このとき、Ｒｉ＋１が実際に正当である確率を、ｆ＿ｐｏｓｔ＿ｒｅｌｙ（Ｒｉ＋１）　と書くと、他に条件がなければ、
ｆ＿ｐｏｓｔ＿ｒｅｌｙ（Ｒｉ＋１）　＝　ｐｉｎｄ（Ｒｉ＋１）／（ｐｉｎｄ（Ｒｉ＋１）＋ｑｉｎｄ（Ｒｉ＋１））　である。
【００５４】
一方、Ｒｉ　が実際に正当である確率を考える。Ｒｉ　はＲｉ＋１　と連鎖しており、また、Ｒｉ＋１　が実際に正当である確率が分かっている。ハッシュ関数の一方向性から、Ｒｉ　が実際に正当であることの事前確率
ｆ＿ｐｒｉ＿ｒｅｌｙ（Ｒｉ）　は、ｆ＿ｐｒｉ＿ｒｅｌｙ（Ｒｉ）　＞＝　ｆ＿ｐｏｓｔ＿ｒｅｌｙ（Ｒｉ＋１）
を満たす。したがって、Ｒｉ　が実際に正当である確率
ｆ＿ｐｏｓｔ＿ｒｅｌｙ（Ｒｉ）は、
ｆ＿ｐｏｓｔ＿ｒｅｌｙ（Ｒｉ）＝　ｆ＿ｐｒｉ＿ｒｅｌｙ（Ｒｉ）　ｐｉｎｄ（Ｒｉ）　／　（ｆ＿ｐｒｉ＿ｒｅｌｙ（Ｒｉ）　ｐｉｎｄ（Ｒｉ）　＋　（１　－　ｆ＿ｐｒｉ＿ｒｅｌｙ（Ｒｉ））　ｑｉｎｄ（Ｒｉ））＞＝　ｆ＿ｐｏｓｔ＿ｒｅｌｙ（Ｒｉ＋１）　ｐｉｎｄ（Ｒｉ）　／　（ｆ＿ｐｏｓｔ＿ｒｅｌｙ（Ｒｉ＋１）　ｐｉｎｄ（Ｒｉ）　＋　（１　－　ｆ＿ｐｏｓｔ＿ｒｅｌｙ（Ｒｉ＋１））　ｑｉｎｄ（Ｒｉ））＝　ｐｉｎｄ（Ｒｉ＋１）　ｐｉｎｄ（Ｒｉ）　／　（ｐｉｎｄ（Ｒｉ＋１）　ｐｉｎｄ（Ｒｉ）　＋　ｑｉｎｄ（Ｒｉ＋１）　ｑｉｎｄ（Ｒｉ））
となる。これを繰り返し適用すればよい。（証明終わり）
命題１より、署名生成記録Ｒｍの信頼度は、上記（式１）の右辺の値で下から評価できることが分かる。したがって、たとえば、上記のステップ８０３６で算出する検証対象となる署名に対応する署名生成記録Ｒｍの信頼度を、上記（式１）の右辺の値とすれば、署名の検証結果を適切に評価することが可能となる。
【００５５】
本実施例に述べた信頼度付きヒステリシス署名検証方法に従えば、署名履歴の信頼度を適切に判定した検証方法が実現可能となる。また、この検証方法に基づいて判定を行うことにより、ヒステリシス署名付きメッセージをめぐる係争を解決する調停方法および調停者装置を提供可能となる。
【００５６】
次に、本発明を署名履歴サービスへ適用する第２実施形態について説明する。
【００５７】
本実施形態におけるシステムの概略図を図１に示す。ただし、本実施形態においては、第１実施形態における履歴管理装置２は各署名者装置１と同一の装置の上で実現されているものとする。また、第１実施形態では説明しなかった、複数の署名者装置１から履歴登録要求を受け付けて署名履歴を保管と管理を行う署名履歴保管サービス装置６と、署名履歴保管サービス装置６に署名者装置１から受信したヒステリシス署名つきメッセージの署名検証代行を依頼する検証代行依頼者装置７とが、履歴管理装置２とは別に、ネットワーク５を介して接続されている。なお、調停依頼者装置３と調停者装置４については、本実施形態では説明しないが、必要に応じて、たとえば第１実施形態と同様の調停者装置を設けてもよい。
【００５８】
図９は、本実施形態における署名履歴保管サービス装置６の構成を示した図である。基本的な構成は、第１実施形態における履歴管理装置２の構成と同様である。
【００５９】
署名履歴保管サービス装置６の外部記憶装置１３に格納されるのは、署名者装置１から登

録を依頼された署名生成記録（ログデータともいう）を受信し、当該署名生成記録を署名生成履歴（ログリストともいう）として登録する履歴登録プログラム（以下、プログラムをＰＧと記す）９０１と、署名者装置１などからの要求に応じて、当該署名履歴保管サービス装置６が管理する署名履歴を送信する履歴送信ＰＧ９０２と、ヒステリシス署名つきメッセージを保持する署名検証代行依頼者からの要求に応じて、署名検証処理を代行して行う署名検証代行ＰＧ９０３と、署名管理装置の利用者の登録処理を行う、利用者登録ＰＧ９０４である。なお、履歴送信ＰＧ９０２は、第１実施形態における履歴送信ＰＧ１３３と基本的に同様である。履歴登録ＰＧ９０１と署名検証代行ＰＧ９０３については、以下の説明の中で詳細に述べる。

【００６０】

上記各プログラムは、ＲＡＭ１２上にロードされ、ＣＰＵ１１が実行することにより履歴登録処理部９１１や履歴送信処理部９１２や署名検証代行処理部９１３や利用者登録処理部９１４というプロセスとして具現化される。外部記憶装置１３には、さらに登録を依頼された署名生成記録を格納するための履歴格納領域９０５が設けられ、署名者ごとに署名履歴（たとえば、ユーザＡ署名履歴９０５１、ユーザＢ署名履歴９０５２）が格納される。

【００６１】

本実施例における署名者装置１の構成は、基本的に第１実施形態の署名者装置１の構成と同様であるが、外部記憶装置１３に格納されるプログラムとして、履歴登録要求ＰＧ１３７が追加されている。

【００６２】

検証代行依頼者装置７も署名者装置１と同様の構成を備える。その外部記憶装置１３に格納されるのは、当該装置７が保持するヒステリシス署名付きメッセージの検証を署名履歴保管サービス装置６に依頼する署名検証要求ＰＧ９０６である。

【００６３】

署名履歴保管サービス装置６と検証代行依頼者装置７が備える各プログラムは、予め外部記憶装置１３に格納されていても良いし、必要に応じて、読取り装置１４を介して記憶媒体１５から、または通信装置１８と通信媒体（すなわちネットワーク５またはそれを伝搬する搬送波）により、他の装置から導入されても良い。

【００６４】

図１０は、本実施例における、署名者装置１が、履歴保管サービスを提供する署名履歴保管サービス装置６に対し、履歴登録を依頼するときの処理フローを示したものである。以下のフローの内、ユーザＡの署名者装置１の処理は、履歴登録要求ＰＧ１３７の実行により、また、署名履歴保管サービス装置６の処理は、履歴登録ＰＧ９０１の実行により実現される。なお以下では履歴登録を依頼する署名者をユーザＡとする。

（ユーザＡの署名者装置１の処理）

ステップ１０００１：はじめ。

ステップ１０００２：登録依頼の意思を示す電子データである「預託依頼書」を作成。

【００６５】

預託依頼書は、登録依頼の意思を示す電子データの他、さらに、時刻情報、ユーザ名、署名者装置１を識別する情報、署名者装置１のネットワークへの接続状況を示す情報（例：ＩＰアドレス）、登録依頼の対象となる署名生成記録の個数や何番目の署名生成記録であるかを示す情報、などを含んで構成されてもよい。

ステップ１０００３：「預託依頼書」に対しヒステリシス署名を生成する。（注：この時点での最新の署名記録、つまりこのステップで生成した「預託依頼書」に対する署名に対応する署名記録がｎ番目の署名記録であったとする。また前回履歴登録依頼をしたときに生成した「預託依頼書」に対応する署名記録がｎ’（＜ｎ）番目の署名記録であったとする。）

ステップ１０００４：ヒステリシス署名付き預託依頼書、預託依頼書の署名生成鍵に対応する公開鍵証明書、ｎ’＋１番目からｎ番目までの署名生成記録が含まれた署名履歴を、

署名管理装置２に送る。
（署名履歴保管サービス装置６の処理）
ステップ１０００５：送られてきた公開鍵証明書の有効性を検証する（有効なＣＡ（認証局）の署名が付与されているか、有効期間内であるか、ＣＡ（認証局）によって無効化されていないか、など）。
ステップ１０００６：送られてきたヒステリシス署名付き預託依頼書が公開鍵証明書に含まれるユーザＡの公開鍵によって正しく検証されるかをチェックする。（ステップ８０３２に示した検証処理が正しく行えるかをチェックする。）
ステップ１０００７：送られてきた署名履歴の整合性検証をチェックする。（ステップ８０３４の処理をｍ＝ｎ’＋１として行う。）
ステップ１０００８：既に保管済みのユーザＡの署名履歴（ｎ’番目までの署名履歴）との整合性をチェックする。（署名生成記録Ｒｎ’のハッシュ値ｈ（Ｒｎ’）　を算出し、署名生成記録Ｒｎ’＋１の中のハッシュ値ｈ（Ｒｎ’）が、算出したｈ（Ｒｎ’）と同じ値であることを確認する。）
ステップ１０００９：ステップ１０００５～１０００８のチェックがＯＫであれば送られてきた署名履歴をユーザＡ署名履歴９０５１に追記する。
ステップ１００１０：ユーザＡに対し、署名履歴（ｎ’＋１～ｎ番目の署名生成記録）を受け付け、整合性を確認し、署名履歴９０５１に追記した旨記された受付確認データ送信する。
（ユーザＡの署名者装置１の処理）
ステップ１００１１：受付確認データを受信する。
ステップ１００１２：ｎ’＋１～ｎ－１番目の署名生成記録を削除する。
ステップ１００１３：おわり。
【００６６】
上記ステップ１００１２は、実行しなくてもよい。実行して一部の署名生成記録を削除すれば、ユーザＡの署名者装置１の記憶領域を節約することができる。ユーザＡの署名者装置１の記憶容量に応じて、削除するか、しないかを選択すればよい。
【００６７】
以上の処理により、履歴保管サービス提供者が、署名者に代わり履歴を保管するため、署名者にとっては署名履歴保管の負荷が削減される（ステップ１００１２）。
【００６８】
なお、ステップ１００１２において、ｎ番目の署名生成記録を削除しないのは、次の署名（ｎ＋１番目の署名））を生成をする際に、ｎ番目の署名生成記録が必要となるからである。
【００６９】
さらに、第三者機関である履歴保管サービス提供者が、署名履歴の連鎖構造に関し整合性を確認し（ステップ１００００７、１００００８）、また、最新の署名である「預託依頼書」に付された署名や対応する公開鍵証明書の有効性を確認するため（ステップ１００００５、１００００６）、登録を要求した署名履歴に対応する署名のうち、預託依頼書に付された署名と同一の鍵を用いて生成されたものについては、公開鍵証明書の有効期間内に生成されたことが保証されるようになる。
【００７０】
上記のフローにおいては、「預託依頼書」を作成し（ステップ１００００２）、ヒステリシス署名を付与し（ステップ１００００３）、ヒステリシス署名付き預託依頼書を送付している（ステップ１００００４）が、これら３ステップを省略してもよい。この場合、ステップ１００００６での署名検証は、ヒステリシス署名付き預託依頼書に対して行うかわりに、送られてきた署名履歴の中の最新の署名記録に対して行う。なお、当該署名記録に対応する署名対象メッセージ自体は署名記録に含まれないが、そのハッシュ値は署名記録に含まれているため、これを用いてステップ１００００６の処理を行うことは可能である。
【００７１】

署名履歴登録要求の頻度については、署名者装置１や署名管理装置２の記憶容量や処理能力あるいは両装置間のネットワーク５に確保できる通信品質状況等に応じて、適切に設定すればよい。一般に、登録要求の頻度が高いほど、署名者装置１の外部記憶装置１３の記憶容量は少なくてすむ。また、署名履歴の信頼度を向上させるという観点からも、登録要求の頻度は高いほうが望ましい。本実施例によれば預託依頼書に付された署名と同一の鍵を用いて生成されたものについては公開鍵証明書の有効期間内に生成されたことを保証できるようになる、という点を考慮すると、署名履歴登録要求の頻度は、公開鍵証明書更新の頻度と同一もしくはそれより高い頻度で行うことが望ましい。ただし登録要求の頻度が高いほど、署名者装置１と署名履歴保管サービス装置６との間の通信回数は多くなる。

【００７２】

署名履歴登録要求の頻度の具体的な一例として、ヒステリシス署名生成のたびごとに、履歴登録要求を行ってもよい。さらに預託依頼書を省略してもよい。このように、ヒステリシス署名生成のたびごとに履歴登録要求を行い、かつ、預託依頼書を省略した場合は、署名者装置１で管理する必要のある署名履歴は最新の署名履歴一つ分だけですむ。したがって、装置の記憶容量の節約と管理負荷の軽減が可能になる。さらに、署名者が生成した署名に対応する署名履歴は、常に署名履歴保管サービス装置６にも存在するという効果も得られる。

【００７３】

さらには、ヒステリシス署名生成の際に必要となるｎ番目の署名生成記録、または、当該署名生成記録のハッシュ値も、必要に応じて署名履歴保管サービス装置６からネットワーク５を介して入手するようにシステムを構成してもよい。このようにすると、署名者装置１での署名履歴の管理が不要となる。あるいは、署名者装置１での署名管理機能を残したまま、署名履歴保管サービス装置６からネットワーク５を介して入手する上記機能を備えるように、システムを構成してもよい。この場合、署名者装置１で管理する署名履歴と、署名履歴保管サービス装置６から入手した署名履歴とを比較して、署名履歴保管サービス装置６において署名履歴の改ざんなど、何らかの不正がなかったかどうかを確認することができるようになる。

【００７４】

また、署名履歴保管サービス装置６において、ｎ番目の署名生成記録を送信するときに、さらに、他の署名者の署名履歴に依存した情報も含めることにより、特開２００１－３３１１０５号公報に開示された、複数署名者の署名履歴を交差させる処理を実現することも可能である。なお、「交差させる」とは、ある署名者の署名履歴の情報を他の署名者の署名履歴に反映させることを意味する。

【００７５】

このように、ある署名者の署名履歴を他の署名者の署名履歴と交差させることは、当該署名が確かに行われたという証拠を分散して持つことに他ならず、署名そのものを偽造しようとしたり、署名が施された時刻情報を改変しようとしたりするときの作業量を増大させ、かつ、それら不正を行うために複数の署名者、または複数の署名者装置を巻き込む必要を生じさせるため、不正を抑止する大きな効果が得られる。

【００７６】

図１１は本実施例における、署名者装置１から受信したヒステリシス署名つきメッセージを保持する署名検証代行依頼者が利用する検証代行依頼者装置７が、署名履歴保管サービス装置６に対し、署名検証代行を依頼するときのフローを示すものである。以下のフローの内、検証代行依頼者装置７の処理は、署名検証要求ＰＧ９０６により、そして署名履歴保管サービス装置６の処理は、署名検証代行ＰＧ９０３により実現される。なお以下の説明では、検証対象となる署名を生成した署名者をユーザＡとする。

（署名検証要求ＰＧ９０６の処理）

ステップ１１００１：はじめ。

ステップ１１００２：ユーザＡのヒステリシス署名付きメッセージを署名履歴保管サービス装置６に対し送信し、署名検証の代行を依頼する。

（署名検証代行ＰＧ９０３の処理）
ステップ１１００３：あらかじめ保管してあるユーザＡの署名履歴を利用し、検証の代行を依頼されたヒステリシス署名付きメッセージの検証を行う。
ステップ１１００４：検証結果を検証代行依頼者装置７に送る。
（署名検証要求ＰＧ９０６の処理）
ステップ１１００５：検証結果を受け取る。
ステップ１１００６：おわり。

【００７７】
上記の処理中のステップ１１００３におけるヒステリシス署名付きメッセージの検証は、第１実施形態に示した「ヒステリシス署名検証処理」と同様にして行えばよい。なお、署名履歴保管サービス装置６を信頼できると考えてよい場合には、ステップ８０３５、８０３６における信頼度の設定、算出は省略して、結果は信頼できるものとみなしてもよい。

【００７８】
さらには、署名履歴保管サービス装置６において、特開２００１－３３１１０５号公報に開示された複数署名者の署名履歴を交差させる機能を実現している場合には、署名履歴交差が正しく行われているかどうかも含めて検証してもよい。

【００７９】
なお、本実施形態では、署名検証代行処理を、履歴登録処理を行う署名履歴保管サービス装置６と同一の装置上で実現する例を示したが、署名検証代行処理は、署名履歴保管サービス装置６と連携した別の装置上に実現されてもよい。

【００８０】
以上に示した本発明の一実施形態においては、署名生成機能は、各署名者が管理する署名者装置１内に設けられていたが、これには限定されない。たとえば、各署名者用の署名生成機能を署名者装置１から分離して、署名履歴保管サービス装置６内に設け、各署名者装置１は、署名履歴保管サービス装置６に対してヒステリシス署名生成を要求し、生成された署名を受け取る機能を設けてもよい。この場合、署名履歴保管サービス装置６には、ヒステリシス署名要求受付時に、パスワードや生体認証技術等により署名者を認証する処理を設けることが望ましい。このように、署名生成機能を第三者機関である署名履歴保管サービス装置６内に設けることにより、署名者にとっては、さまざまな署名者装置を利用して自身の署名を生成できるようになる。たとえば、署名者が複数のＰＣ（Ｐｅｒｓｏｎａｌ　Ｃｏｍｐｕｔｅｒ）、携帯電話、ＰＤＡ等の装置を所有している場合、どの装置からでも自身の署名を生成できることになる。

【００８１】
以上に示した第２の実施形態においては、署名者に代わり、署名者が作成した署名履歴を長期にわたり信頼性の高い状態で保管する署名履歴保管サービスを提供することが可能となる。さらに、署名履歴を利用した署名検証処理を代行する署名検証代行サービスを提供することが可能となる。

【００８２】
なお、上記第２の実施形態の各装置は、他の装置の機能を併せて備え、必要に応じて、異なる装置として機能してもよい。

【００８３】
また、上記第１、第２の実施形態において、各装置が備える各プログラムは、予め外部記憶装置に格納されていても良いし、必要に応じて、読取り装置を介して記憶媒体から、または通信装置と通信媒体（すなわちネットワークまたはそれを伝搬する搬送波）により、他の装置から導入されても良い。

【００８４】
【発明の効果】
本発明によれば、署名履歴の信頼度を適切に反映するように構成された検証方法を提供することが可能となる。また、この検証方法に基づいて署名の正当性をめぐる係争を解決する調停方法および調停者装置が提供可能となる。

【図面の簡単な説明】

【図１】本発明の実施形態が適用されたシステムの概略図である。

【図２】署名者装置１、履歴管理装置２、調停依頼者装置３、調停者装置４の概略構成を示した図である。

【図３】署名者装置の署名付きメッセージ作成ＰＧ１３１の処理フローを示す。

【図４】履歴管理装置の履歴登録ＰＧ１３２の処理フローを示す。

【図５】履歴管理装置の履歴送信ＰＧ１３３の処理フローを示す。

【図６】調停依頼者装置の履歴要求ＰＧ１３４の処理フローを示す。

【図７】調停依頼者装置の調停依頼ＰＧ１３５の処理フローを示す。

【図８】調停者装置の調停ＰＧ１３６の処理フローを示す。

【図９】署名履歴保管サービス装置６の概略構成を示した図である。

【図１０】第２実施形態において署名者装置１が署名履歴保管サービス装置６に対し履歴登録を依頼するときのフローを示す。

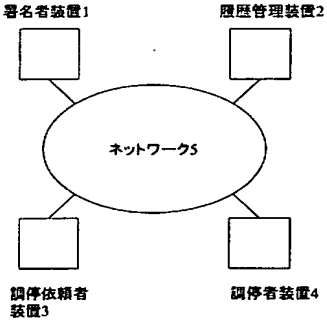
【図１１】第２実施形態において検証代行依頼者装置７が署名履歴保管サービス装置６に対し署名検証代行を依頼するときのフローを示す。

【符号の説明】

１…署名者装置、２…履歴管理装置、３…調停依頼者装置、４…調停者装置、６…署名履歴保管サービス装置、７…検証代行依頼者装置、１１…ＣＰＵ、１２…ＲＡＭ、１３…外部記憶装置、１４…読取装置、１５…可搬性記憶媒体、１６…入力装置、１７…表示装置、１８…通信装置、２０…インターフェイス、２１…電子計算機、１３１…署名付きメッセージ作成ＰＧ、１３２…履歴登録プログラム、１３３…履歴送信プログラム、１３４…履歴要求プログラム、１３５…調停依頼プログラム、１３６…調停プログラム、１３７…履歴登録要求プログラム、９０１…履歴登録ＰＧプログラム、９０２…履歴送信プログラム、９０３…署名検証代行プログラム、９０４…利用者登録プログラム、９０５…履歴格納領域、９０６…署名検証要求プログラム、１３７…履歴登録要求プログラム。

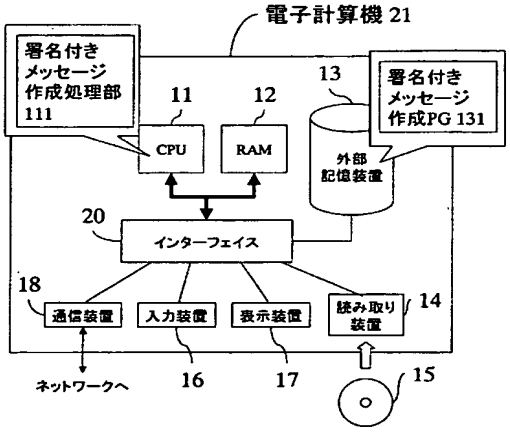
【図１】

図1



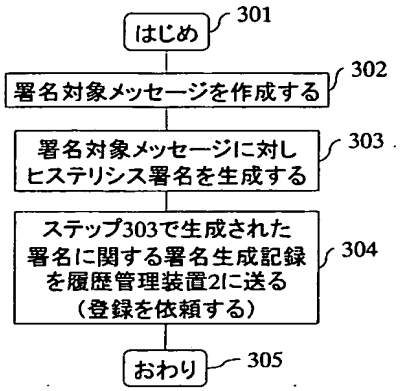
【図２】

図2



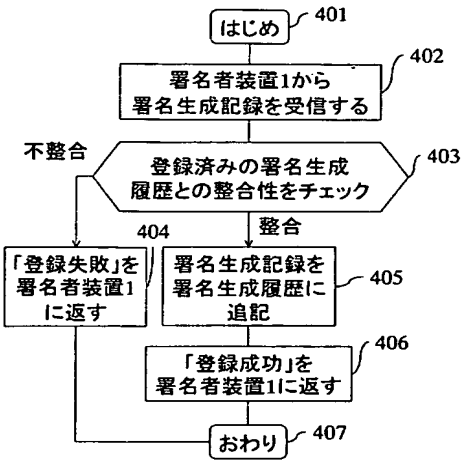
【図３】

図3



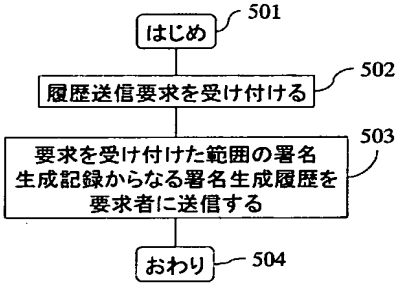
【図４】

図4



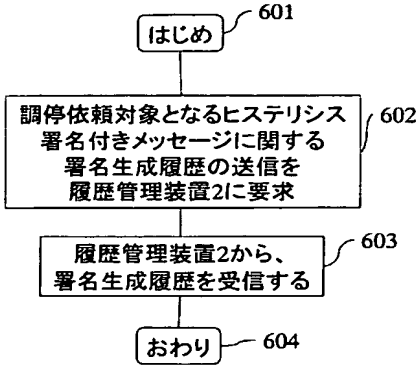
【図５】

図5



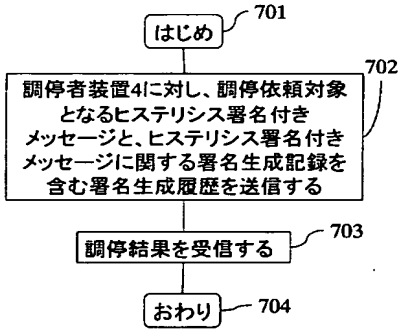
【図６】

図6



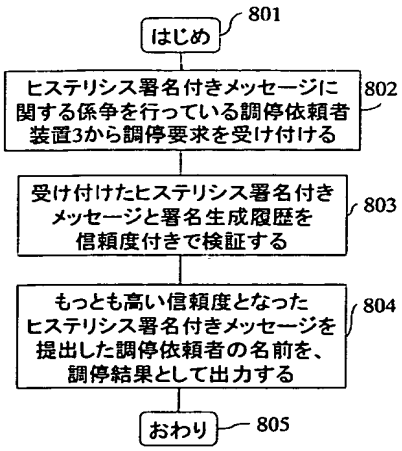
【図７】

図7



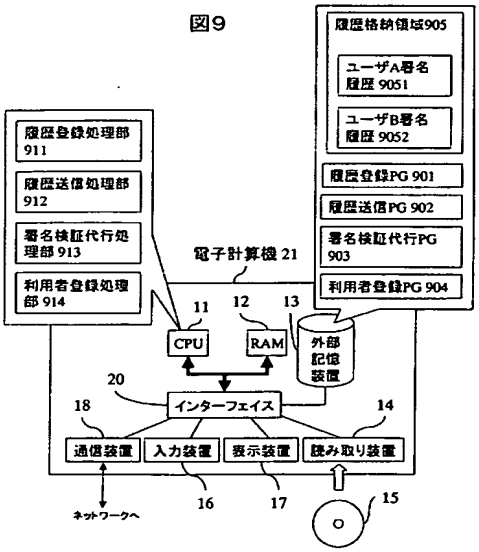
【図８】

図8



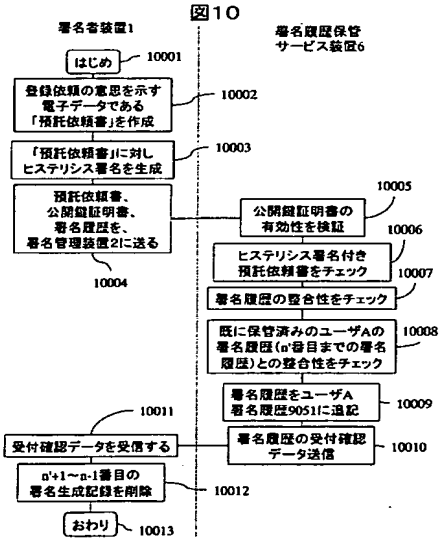
【図９】

図9



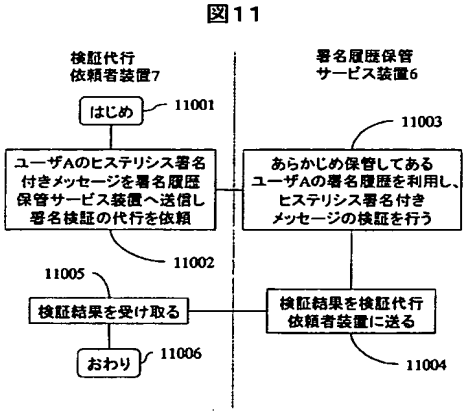
【図１０】

図10



【図１１】

図11



フロントページの続き

(72)発明者 伊藤 信治
神奈川県川崎市麻生区王禅寺１０９９番地 株式会社日立製作所システム開発研究所内
(72)発明者 谷本 幸一
神奈川県川崎市麻生区王禅寺１０９９番地 株式会社日立製作所システム開発研究所内
(72)発明者 吉浦 裕
神奈川県川崎市麻生区王禅寺１０９９番地 株式会社日立製作所システム開発研究所内

Fターム(参考) 5J104 AA08 LA03